

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Hon. Hugh B. Scott

v.

11CR397S

**Report &
Recommendation**

James Raymonda,

Defendant.

Before the Court is the defendant's motion to suppress evidence (Docket No. 9).

Background

The defendant, James Raymonda ("Raymonda"), was indicted on December 21, 2011 on charges that he received child pornography on or about January 16, 2011 in violation of 18 U.S.C. §2252A(a)(2)(A) [Count 1]; and that he possessed child pornography on November 8, 2011 in violation of 18 U.S.C. §2252A(a)(5)(B) [Counts 2-5]. The Indictment also includes forfeiture allegations relating to various computer equipment. (Docket No. 5).

The charges against Raymonda arise from an investigation commencing in or about January of 2011. The defendant argues that the evidence obtained as a result of a search of 73 Henley Road in November of 2011 must be suppressed inasmuch as the warrant application was based upon stale information, and therefore, probable cause did not exist. The defendant also

seeks suppression of any statements he made to the police at the time of the search. (Docket No. 9).

A suppression hearing in this matter was commenced on August 7, 2012 and continued on several dates. Adam Ouzer, a special agent with Homeland Security Investigations (“HSI”) testified that on October 3, 2011 he received information from the HSI office in San Diego that in January of 2011 they commenced an investigation of child pornography on a website called “Motherless” which was linked to another website called “Coolib” (Docket No. 26 at 8-9). Ouzer testified that the information obtained from the HSI San Diego office indicated that an IP address, 67.252.174.8 [“IP address”], assigned to a computer located in Buffalo, New York had accessed the Motherless website. (Docket No. 26 at 16). Ouzer was able to determine that the subscriber of that IP address was Raymonda, and he verified that Raymonda lived at 73 Henley Road in Buffalo, New York. (Docket No. 26 at 16-17).¹ Referring to the “get codes” contained in the IP log [Government’s Exhibit 4], Ouzer testified that the information received from San Diego reflected that the IP address “clicked” 76 thumbnail² images to enlarge them on the computer on January 16, 2011. (Docket No. 26 at 18-19). Ouzer stated that the information from the San Diego HSI included copies of images taken from the Motherless and Coolib websites which correspond to the “get code” information contained in the IP log allegedly listing the

¹ Ouzer testified that, among other things, he checked New York State Division of Motor Vehicle records and conducted surveillance of 73 Henley Road on October 13, 2011, October 20, 2011 and November 7, 2011. He observed Raymonda’s wife leave for work; and using binoculars, observed a male inside the house. (Docket No. 26 at 63-65)

² Ouzer testified that a “thumbnail” image is approximately “an inch by an inch” (Docket No. 26 at 95) and that they are smaller images that you can click on to obtain a larger image of what is depicted in the thumbnail. (Docket No. 26 at 94).

images accessed by Raymonda. Ouzer testified that these images included images of minors under the age of 18 engaged in sexually explicit conduct. (Docket No. 26 at 21). Using this information, Ouzer applied for a search warrant (Government's Exhibit 5) on October 27, 2011. (Docket No. 26 at 22). He, and other agents, executed the search warrant on November 8, 2011 – approximately 10 months after the date that the images had allegedly been accessed by Raymonda.

With respect to the search of 73 Henley, Ouzer stated that he and the other agents, between 8 and 10 officers (Docket No. 26 at 83), arrived at the single family house just before 7:00 am on November 8, 2011. The officers set up around the perimeter of the house, and Ouzer knocked on the back door, announced their presence and stated that they had a search warrant. Ouzer stated that Raymonda opened the door. (Docket No. 26 at 22-23, 84-85).³ According to Ouzer, the officers first searched the house for “threats.” The defendant's wife and two infant children were home at that time. (Docket No. 26 at 24). After the house was “cleared” for threats, Ouzer stated that he asked Raymonda if he would step outside so they could talk to him. Ouzer testified that the house was cluttered and noisy, and at least one of the children was crying. (Docket No. 26 at 24). Ouzer, Special Agent Christopher Bennett and Raymonda proceeded outside to Bennett's unmarked Ford Explorer.⁴ Raymonda allegedly walked toward the front passenger side of the vehicle, while Ouzer went to the driver's side. Bennett sat behind

³ HSI Special Agent Christopher Bennett testified that the officers approached the front door and that Raymonda's wife was at that door. (Docket No. 26 at 113).

⁴ Ouzer and Bennett testified that they had intended to interview all the adults in the house and that they had not yet targeted Raymonda prior to the interview. (Docket No. 26 at 89-90, 134).

Raymonda on the passenger side of the vehicle. The doors of the vehicle were not locked (Docket No. 26 at 35). Ouzer stated that Raymonda hit his head on the car door when entering, causing Raymonda to bleed. (Docket No. 26 at 25-26).⁵ Ouzer stated that Raymonda declined any medical attention. According to Ouzer, Raymonda had been provided with a copy of the search warrant and Ouzer asked Raymonda if he wanted time to read the warrant or if he wanted them to explain the warrant. (Docket No. 26 at 26-27). Ouzer testified that Raymonda asked them to explain the warrant, so Ouzer advised Raymonda that it was a search warrant only, not an arrest warrant and that they did not have the intention to arrest anyone that day. Ouzer stated that he explained to Raymonda that they were looking for evidence of child pornography. (Docket No. 26 at 27-28). Ouzer stated that he advised Raymonda that he could leave the residence or he could stay at the residence, but if he stayed inside the residence, an agent would need to stay with him for officer safety. (Docket No. 26 at 27). Raymonda allegedly chose to stay and Ouzer asked Raymonda if he could ask him some questions, to which Raymonda agreed. (Docket No. 26 at 27). During the conversation, Raymonda allegedly told Ouzer that there were two desktop computers, two laptop computers and various forms of electronic media inside the house. Ouzer testified that Raymonda stated that he knew child pornography was illegal. When asked by Ouzer if he had ever accessed the Motherless and “4chan” websites⁶, Raymonda allegedly responded that he had accessed these websites. (Docket No. 26 at 29-30). Ouzer stated that they showed Raymonda “a picture of the actual board that prompted this investigation” and

⁵ Ouzer testified that Raymonda opened and closed the door to the vehicle on his own. (Docket No. 26 at 26).

⁶ According to Ouzer, “4chan” is another website containing child pornography that the agents have encountered in previous investigations. (Docket No. 26 at 29).

asked Raymonda if it looked familiar to him and he said it did. (Docket No. 26 at 30). Ouzer then showed Raymonda other images purportedly from the websites in question, and Raymonda allegedly indicated that he remembered some of them. Ouzer stated that Raymonda told him that child pornography was not something he looked at every day, but acknowledged accessing at least one of the websites that morning. (Docket No. 26 at 31-32). Ouzer testified that he asked Raymonda “if he would log on, download or look at child pornography, masturbate, and then log off, and he agreed to that statement.” (Docket No. 26 at 32). Raymonda purportedly told Ouzer that when he looked at the images of child pornography, he would think “what the fuck am I doing.” (Docket No. 26 at 32). Ouzer allegedly asked Raymonda if he knew what the search term “PTHC” stood for and Raymonda responded “pre-teen hard core.” (Docket No. 26 at 33).

Ouzer stated that the interview with Raymonda took approximately one half hour; they thanked Raymonda for cooperating with them and told him that he was free to go. (Docket No. 26 at 34). It is undisputed that Raymonda was not advised of his rights pursuant to Miranda v. Arizona, 384 U.S. 436 (1966) at any time during the interview. (Docket No. 26 at 91). Ouzer testified that during the interview Raymonda provided appropriate answers to the questions asked; he was oriented to what was being discussed; he was not restrained in any way; he was not handcuffed; he did not ask to have an attorney; he did not ask to stop the interview. (Docket No. 26 at 44-45). Ouzer stated that he did not take out his weapon, but acknowledged that agents first entering the building would have had their firearms out, and that these weapons would have been holstered as soon as the house was secured. (Docket No. 26 at 46-47). Ouzer testified that neither he nor Bennett grabbed Raymonda’s arm or touched him. (Docket No. 26 at 47). Ouzer

stated that Raymonda asked when he would get the computer parts back. (Docket No. 26 at 45).⁷

While Ouzer, Bennett and Raymonda were in the vehicle talking, other agents had been executing the search warrant. Ouzer, Bennett and Raymonda went back into the house. (Docket No. 26 at 35). Once back inside the house, according to Ouzer, Raymonda was “more upset than he was when [they] were inside the vehicle” and he went up to Ouzer and stated that he wanted Ouzer to “put a bullet in his head, and that his life was over and he had lost everything.” (Docket No. 26 at 36-37). Ouzer said that he had learned from other agents that Raymonda made that statement to him just after Raymonda’s wife had just informed Raymonda that she was “leaving with the kids.” (Docket No. 26 at 39). In light of these statements by Raymonda, an ambulance was called for and Raymonda was transported for a mental health evaluation. (Docket No. 26 at 40-41).⁸ Ouzer testified that several items were seized pursuant to the search warrant, including multiple computers, multiple forms of electronic media (such as USB drives) and a camera. According to Ouzer, an analysis by a forensic agent revealed several “files which meet the definition of 18 U.S.C. §2256, child pornography.” (Docket No. 26 at 43).

On cross-examination, Ouzer acknowledged that the information in the search warrant application, particularly the “get codes” in the IP log, would only demonstrate that “thumbnail”

⁷ In an affidavit dated April 11, 2012, Raymonda alleges that in the early morning of November 8, 2011, several police cars pulled up to his home. According to the defendant, “[o]ne of the officers told me, ‘Come outside with us’ and he put his arm on me and lead me to their police car.” (Docket No. 12-1 at ¶ 3). Raymonda testified that as he entered the police vehicle, he hit his head and it started bleeding; that he was “extremely upset” and “felt like I had to speak to them” (Docket No. 12-1 at ¶¶3-4)

⁸ The ambulance was called for by the Buffalo Police Officers present on the scene. Ouzer and Bennett testified that Raymonda did not resist going in the ambulance for the mental evaluation. (Docket No. 26 at 42, 126)

images from the websites in question were automatically downloaded into a temporary internet directory or cache of the user's computer and that the "get codes" do not reflect that any larger versions of the image were received by the computer. (Docket No. 26 at 52-57). Ouzer stated that the information in the search warrant only reflects that the images were "asked for" and does not indicate that they had been successfully downloaded onto the computer. (Docket No. 26 at 51-53). Further, Ouzer acknowledged that there is a fixed amount of cache space on a computer and that files are overwritten as they are replaced with more recently viewed internet pages. (Docket No. 26 at 56). The search warrant application in this case does not reflect that the plaintiff used any peer-to-peer file sharing applications to view or trade images of child pornography. (Docket No. 26 at 57). Although Ouzer's affidavit in support of the search warrant stated that "the persons residing at the subject premises exhibits the common characteristics ... of someone involved in the distribution, receipt, and possession of child pornography," (Government's Exhibit 4 at ¶35), Ouzer admitted that there was no evidence in the investigation at that point that Raymonda was involved in the distribution of child pornography. (Docket No. 26 at 60). Ouzer also admitted that, at the time he applied for the search warrant, it was possible that the images reflected in the "get codes" as having been automatically downloaded into the internet cache of Raymonda's computer had already been overwritten. (Docket No. 26 at 61).

Bennett's suppression hearing testimony relating to the discussion between Ouzer and Raymonda in Bennett's vehicle is consistent with Ouzer's testimony. (Docket No. 26 at 114-124). Bennett stated that he took notes during the interview (Government's Exhibit 6). Jeffrey Jajkowski, an officer with the Buffalo Police Department, also testified at the suppression hearing. He stated that he was advised of the statements allegedly made by Raymonda to the

effect that Raymonda asked a federal agent to put a bullet in his head because his life was over. Jajkowski testified that pursuant to the New York State Mental Health Law, the police have the authority to send people to the Erie County Medical Center for psychological evaluation if they believe the person may harm themselves. (Docket No. 26 at 149). According to Jajkowski, he asked dispatch to send an ambulance; the ambulance arrived; Raymonda agreed to enter the ambulance on his own free will and Raymonda was taken to ECMC. (Docket No. 26 at 151).

Raymond argues that because Ouzer had been the case agent involved in another case involving child pornography in this District, United States v. Coon, No. 10CR110, Ouzer was aware that the information he used to obtain the search warrant in this case was stale and that probable cause was lacking. In Coon, on May 16, 2011, after extended proceedings regarding the suppression issue, Hon. Richard J. Arcara determined that the information contained in the application for a search warrant (which was almost one year old) was stale; that probable cause did not exist for the search warrant; but that suppression of the evidence was not required under the good faith exception to the exclusionary rule.⁹ It is undisputed that Ouzer was the case agent

⁹ The chronology relating to the motion to suppress in Coon is as follows: Coon filed a motion to suppress on **June 21, 2010** (Coon, No.10CR110; Docket No. 19); oral argument was held before the undersigned on **July 16, 2010** (Coon, No.10CR110; Docket No. 24); on **August 20, 2010** the Court determined that an evidentiary hearing was necessary relating to the good faith exception under United States v. Leon, 468 U.S. 897 (1984); the motion was to take place on **September 20, 2010** (Coon, No.10CR110; Docket No. 25); on **September 10, 2010**, the government filed a motion for reconsideration regarding the need for a hearing (Coon, No.10CR110; Docket No. 28); further oral argument on the motion for reconsideration was held before the undersigned on **October 7, 2010** (Coon, No.10CR110; Docket No. 31); on **November 8, 2010**, the Court issued a Report & Recommendation denying the motion to suppress (Coon, No.10CR110; Docket No. 33); Coon filed objections to the Report & Recommendation on **November 23, 2010** (Coon, No.10CR110; Docket No. 34); the government filed a response to the objections on **March 16, 2011** and **April 6, 2011** (Coon, No.10CR110; Docket Nos. 35 & 37); oral argument with respect to the objections to the Report & Recommendation was held on **April 11, 2011** before Judge Arcara (Coon, No.10CR110; Minute Entry dated April 11, 2011);

who obtained the search warrant in Coon. (Docket No. 26 at 101). However, Ouzer testified that he was not aware that the undersigned or Judge Arcara had ruled that the information in the search warrant application in Coon was stale or that probable cause did not exist for the warrant. (Docket No. 26 at 76-77). The defendant called Vincent J. Salvatore, Assistant Special Agent in Charge of HSI in Buffalo, to testify at the suppression hearing. He stated that he did not review search warrant applications which were drafted by the agents working directly with the Assistant United States Attorney working on the case. (Docket No. 28 at 182). Salvatore stated that upon being placed in a supervisory role over Ouzer (and other agents) in August of 2011, he reviewed the cases Ouzer had been working on at that time, including the Coon case. (Docket No. 28 at 184). As of August 2011, however, Salvatore stated that he was not aware that either the undersigned, nor Judge Arcara, had found that the information in Ouzer's search warrant application in the Coon case was stale. (Docket No. 28 at 184). The record reflects that on September 19, 2011 – approximately one month before Ouzer made the application for a search warrant in the instant case – Salvatore sent an email to his supervisor, Michael J. Kennedy, advising Kennedy that Coon had pled guilty and stating that he thought Ouzer did a “nice job” in the Coon case. The email includes an outline regarding the significant events of the investigation; the issuance of the search warrant; the issuance of an arrest warrant; the results of the forensic analysis; Coon's arrest on September 29, 2009; and his guilty plea on September 11, 2011. (Defendant's Exhibit F). According to Salvatore, these “significant event” entries which

on **May 16, 2011** Judge Arcara issued a Decision & Order declining to adopt the Report & Recommendation, finding that probable cause did not exist for the search warrant but that suppression was not required pursuant to the good faith exception. (Coon, No.10CR110; Docket No. 43).

appear below the text of his email to Kennedy would have been added by another individual, possibly Ouzer. (Docket No. 28 at 206-207). The government called Nicholas DiNicola, also an Assistant Special Agent with the HSI who was Ouzer's supervisor for a portion of the time Ouzer worked on the Coon case. Notes by DiNicola state that he reviewed the status of the Coon case with Ouzer and at one point had a discussion with Ouzer about "an ongoing suppression hearing." (Docket No. 30 at 250; Defendant's Exhibit G). DiNicola stated that when doing a case review, he would have looked "at the whole case file" and that if a judge were to have directed that a good faith hearing was required in a case to determine whether evidence would be suppressed, that "it most likely would be discussed." (Docket No. 30 at 255). Notwithstanding, DiNicola stated that he did not review the Court file in the Coon case when he sat down to review the case with Ouzer. (Docket No. 30 at 267). Finally, Assistant United States Attorney Edward H. White testified at the suppression hearing. White was the prosecutor that worked with Ouzer in the Coon case. (Docket No. 30 at 272-273). White stated that the Coon case originated from a referral by the Federal German police that had discovered Coon's IP address in connection with a child pornography investigation in Germany. (Docket No. 30 at 273). White recounted the procedural history relating to Coon's motion to suppress the evidence obtained pursuant to the search warrant in that case, leading to Judge Arcara's decision that the search was based upon stale information. (Docket No. 30 at 275-277; Defendant's Exhibit C). As to whether White had any recollection of conversations with Ouzer about the proceedings leading up to Judge Arcara's ruling, White testified:

Yeah, I don't have a real – any specific recollection of a specific conversation that I had with Agent Ouzer. The best that I can recall is that I – it's just my general practice, I assume – I'm sure that I

generally kept the agent, Agent Ouzer, kind of up to date on where we stood in the briefing cycle, either through telephone conversations or through e-mail. But I don't have any specific recollection of having a specific conversation with him.

(Docket No. 30 at 277). White testified that he recalled asking Ouzer for additional factual information regarding how the case was first referred to ICE and how it ended up being referred to the Western District of New York when drafting the briefs involved in the Coon case. (Docket No. 30 at 278). White stated that a trial was scheduled to take place in the Coon case in September of 2011, and that he worked with Ouzer and a forensic expert to prepare for the trial during the summer of 2011. (Docket No. 30 at 279-280). When asked if he had notified Ouzer of Judge Arcara's decision relating to the suppression motion in May of 2001, White stated:

I don't recall specifically having a conversation or notifying Agent Ouzer about the decision, but I'm fairly confident that I would have, because it was a significant decision. And I think at the most I – I'm sure I would have said look, okay, the pretrial motions are done, the defendant's motion to suppress was denied, and now we're looking at trial.

(Docket No. 30 at 280). When asked if he specifically discussed the "staleness" issue with Ouzer, White testified:

I don't have a specific recollection of ever sitting down with Agent Ouzer and discussing like the staleness issue. I think, again, I'm sort of speculating. ... I think the most detail that I would ever have gone into with Agent Ouzer on it was to say one of the issues raised is staleness, that in the Coon case that the defendant is alleging that the search warrant was stale, that too much time had passed from the date of when the German police downloaded the video to the time when we got the authorization for the search warrant. And I think that's about the extent of it.

(Docket No. 30 at 282). White was asked about e-mail communications between him and Ouzer on March 12, 2011 and March 14, 2011. In the March 12, 2011 e-mail, White asked Ouzer to

provide further information regarding when the German authorities first requested assistance; when a summons was sent to Verizon for information; when Verizon responded to the summons; and when Ouzer did a public records check on the Coons. In this regard, White's e-mail to Ouzer stated: "I suspect that much of this activity occurred over the 11 month time frame from the time when the [German authorities] first downloaded the CP video on 4/11/08 to the time we applied for the search warrant on 3/31/2009." (Defendant's Exhibit I). When asked about this e-mail at the suppression hearing, White stated that it was "fair to say that I thought Agent Ouzer ... understood that this was in connection with Jeff Coon's motion asserting that there was a staleness issue." (Docket No. 30 at 305). White testified that there was no suppression hearing in Coon, and that all the proceedings were done on paper. (Docket No. 30 at 288). On cross examination, White acknowledged that a hearing relating to the good faith issue was scheduled by the Court. (Docket No. 30 at 294). When asked if he notified Ouzer of the impending hearing, inasmuch as he would have called Ouzer as a witness at the hearing, White testified that "I can't recall. I would assume that at some point I'm sure I did." (Docket No. 30 at 294). The good faith hearing did not take place because the government filed a motion seeking reconsideration of the determination to have a hearing. (Docket No. 30 at 294).

Notwithstanding, White testified that he does not believe that he told Ouzer about Judge Arcara's finding that the information in support of the warrant in that case was stale, stating "I don't believe I got into the weeds of what the decision entailed." (Docket No. 30 at 308). White stated that "if I would have said anything, it would have been he [Judge Arcara] found that the warrant was stale, but up – but found the good faith exception applied, so he denied the motion to suppress." (Docket No. 30 at 309).

The defendant also called Gerald R. Grant, Jr. to testify at the suppression hearing. Grant is a certified forensic investigator for the Federal Public Defender's Office. (Docket No. 28 at 211). Grant testified regarding the IP Log (Government's Exhibit 4) and the "get codes" contained therein. According to Grant, the IP Log reflects that on January 16, 2011, IP address 67.252.174.8 issued a "get command" which resulted in a series of entries on the IP Log starting at 7:03:16 and ending at 7:03:33 – a period of 17 seconds of activity. (Docket No. 28 at 218). Grant testified that if a person clicks "on a page with 30 pictures, but some of them finished [loading] faster than other, then they would get an earlier time stamp, and then the other ones would continue downloading until they were successful, or failed in some way, and the log would show that. [The various time stamps between 7:03:16 and 7:03:33 are not] an indication that somebody is clicking exactly on those seconds, it's when the completion of the request is done." (Docket No. 28 at 229). Grant stated that the "get commands" indicate that a web page was accessed "showing" various pictures on the screen to the user. He stated that the files, attachments or links are copies to the computer's internet cache, which Grant referred to as a "temporary holding area" on the computer. According to Grant, these images remain in the cache until they are deleted on a first-in-first-out ("FIFO") basis when the cache become full. (Docket No. 26 at 220). Grant stated that the average length of time that a file would remain in the cache varies "anywhere from two days to a month" on cases he has dealt with. (Docket No. 28 at 221). Grant testified that the IP Log identified as Government's Exhibit 4 contains nothing that would suggest anything other than the user viewed pictures in the internet web browser. According to Grant, there is no information in Government's Exhibit 4 that would indicate that the user saved any child pornography to his computer. (Docket No. 28 at 221). Grant explained:

Just because a line says that there's a get command and a picture was completed, there would be no indication on the server to find out what really happened on the user end. For example, if I clicked on it and there were a number of pictures on this page, but my browser window was very tiny, or I never scrolled, I could see one picture or even a part of a picture, and there could be 30 other pictures below my window, it would still give the same log file as if there were all looked at on the computer, But forensically, there's no distinction, because you cannot tell if a person scrolled up or down or actually viewed the entire web page. The could simply close it, and it would indicate the exact same log.

(Docket No. 28 at 222). Grant stated that it would be impossible to view 76 images in 17 seconds. (Docket No. 28 at 222). Grant testified that somebody could have clicked on one picture and received the 76 entries that are depicted in the IP Log (Government's Exhibit 4). (Docket No. 28 at 223). Grant stated that the information in the IP Log does not indicate what pictures were viewed;¹⁰ does not indicate how long any pictures were viewed; does not indicate what was done with the pictures that were viewed on the website; and does not indicate that the pictures were saved or shared. (Docket No. 28 at 223). On cross-examination, Grant acknowledged that for the time period that the images remained in the internet cache, a person "with enough knowledge" could access them and move them to a different area on the computer. (Docket No. 28 at 231).

¹⁰ The government does not contend that all of the 76 images identified in the IP Log constituted child pornography.

Probable Cause for the October 27, 2011 Warrant

Raymonda argues that probable cause did not exist to support the issuance of the October 27, 2011 search warrant. A review of the search warrant application reveals that the first 14 pages of the search warrant affidavit by Ouzer defines various terms used in the affidavit and general information regarding the seizure of computers and the internet. (Government's Exhibit 5, ¶¶ 6-24). Ouzer then provides information regarding the Motherless website and some of the pornographic images of children posted on the website by individuals identified as "edangle" and "anonymous." (Government's Exhibit 5 at ¶26). The affidavit does not tie these images to Raymonda in any way. Ouzer provides information regarding the investigation by the HSI in San Diego and the link between the Motherless website and the www.coollib.org website. (Government's Exhibit 5 at ¶¶ 27-29). In terms of specific information relating to Raymonda, Ouzer states that web access logs from www.coollib.org included the IP address 67.252.174.8. Ouzer states that "there is no record that the user accessed an enlarged (full size) image" but that the logs show "more than one incidence of access of thumbnail images by the user." (Government's Exhibit 5 at ¶ 30). Ouzer states that information from Time Warner Cable revealed that the IP address was registered to Raymonda (Government's Exhibit 5 at ¶31); that the IP log revealed that the suspect viewed thumbnails of child pornography images (Government's Exhibit 5 at ¶32); and that the access logs reflect that 76 images, the majority of which constituted child pornography, were accessed by the user. (Government's Exhibit 5 at ¶33). The remaining paragraphs of the affidavit relate generalized information about characteristics common to individuals involved in child pornography; procedures relating to electronically stored information and other general information regarding the seizure, retention

and extraction of electronic data. (Government's Exhibit 5 at ¶¶ 34-37).

Initially, the Court finds that the records obtained by HSI which are summarized in the warrant application do not reflect that there was more than one incident of access by the user or that the user accessed 76 separate images. The Court finds the testimony of Grant credible to the effect that the IP Log reflects that the images were downloaded over a 17-second period into the internet cache of the user's computer, and that all 76 of the get commands could have been generated by one click on the webpage at issue. Moreover, the records in this case (See IP Log, Government's Exhibit 4) only reflect that the user accessed the Motherless website on one occasion, on January 16, 2011, and do not reflect "more than one incidence of access of thumbnail images by the user" as stated by Ouzer in the search warrant affidavit. The Ouzer affidavit is also misleading to the extent that it states that there was evidence to suggest that the person residing at 73 Henley was involved in the "distribution" of child pornography. (Government's Exhibit 5 at ¶35). The Court also notes that there is an absence of corroborative information demonstrating Raymonda's involvement in child pornography. There is no assertion that Raymonda used peer-to-peer software to view or share child pornography. There is no information from confidential sources implicating Raymonda's involvement with child pornography. There is no evidence that Raymonda chatted with other on the child pornography websites. There was no evidence to suggest that Raymonda was a pedophile or that he was engaged in on-going criminal conduct. No evidence was presented in support of the search warrant to the effect that any non-thumbnail images were accessed; that any images were saved on the user's computer outside of the internet cache; or that any images were uploaded to the website by the user. The only evidence specific to the as of then unidentified user proffered in

support of the October 27, 2011 search warrant was the almost 10-month old information that on one day in January of 2011, the user of the IP address 67.252.174.8 accessed the Motherless website, and that various thumbnail images were automatically downloaded into the internet cache of the user's computer. No evidence was proffered to demonstrate that the images downloaded into the internet cache of the user's computer would still be in the cache almost 10-months later. In this regard, the Court credits the testimony of Grant to the effect that the internet cache on a typical computer has limited capacity and that once the cache is filled the information in the cache is deleted and replaced with new information automatically downloaded during any internet usage.

The information provided in support of the search warrant in the instant case is less compelling than the evidence presented for the search warrant in Coon. In Coon, the German authorities had downloaded a video containing child pornography *from* an IP address traced back to Coon's residence in Niagara Falls, New York. (No.10CR110; Docket No. 43 at page 2). Coon's computer was the alleged *source* of the child pornography at issue in that case. Thus, there was evidence that the child pornography was, at least at some point in time, contained on that computer in a more permanent location than the internet cache. However, inasmuch as more than 10-months had passed between the time the German authorities downloaded the video and the date of the search warrant application in the United States, the Court in Coon determined that the information was stale. In this regard, Judge Arcara stated:

Turning to the merits of the staleness argument, numerous courts have recognized that digital files remain on computers for extensive periods of time, even if they have been deleted. As the government correctly notes, forensic experts can often recover deleted computer files. For this reason, many courts have suggested

that the staleness issue in the context of digital evidence is somewhat unique, and the passage of time does not necessarily render the evidence stale. ... However, the ability to recover deleted computer files does not, without more, support probable cause to search a residence. There also must be probable cause to believe that the computer will be located at the residence at the time of the search. Ordinarily, where the time between the downloading of the pornography and the search of the residence is relatively brief, it is easy to infer that the computer is still at the location where the pornography was downloaded. The shorter the time between those two events, the stronger the inference. Conversely, as more time passes between the initial download and the search of the residence, the more attenuated probable cause becomes.

In this case, almost an entire year had elapsed from the time that German authorities initially discovered the child pornography and the time that his residence was searched. During that period, no additional illicit downloads occurred. No new information was discovered, except that agents confirmed that the name on the Verizon account matched the name on the utility records for the residence.² This information confirmed to the agents that the person living at the residence was likely the same person who downloaded the child pornography. However, the defendant correctly points out, nothing about that information confirmed to the agents that [the] computer would still be located at the defendant's address.

(Coon, No.10CR110; Docket No. 43, pages 5-6)(citations omitted)

In the instant case, as noted above, almost 10-months had passed between the time that the HSI investigators in San Diego identified Raymonda's IP address as having accessed the Motherless website, and the date of the search warrant application at issue. In addition to all of the deficiencies noted by Judge Arcara in Coon, the application for the search warrant in the instant case had the additional infirmity in that the information presented only established that the images in question had been automatically loaded into the internet cache of the user's computer. The government presented no information demonstrating that the images at issue were permanently saved on the user's computer. Thus, these images were subject to automatic

permanent deletion as the cache received new information from any internet usage. As noted above, the testimony of Grant, the defendant's proffered expert, states that information would remain in a typical internet cache between 2-days and 1-month before being deleted with new incoming internet data. This testimony is unrefuted in the record. If the Court were to assume that the information would remain in the internet cache as much as five times longer than estimated by Grant, the images identified in the IP Log in this case would still have long been deleted prior to the issuance of the search warrant in this case. The Court concludes that the information presented in support of the search warrant in this case was stale and uncorroborated.

As in Coon, the government here argues that any evidence that an individual has viewed an image containing child pornography via the internet provides probable cause to believe that the individual collects and hoards child pornography. With respect to this argument, Judge Arcara held:

Recognizing this deficiency, the government asks this Court to infer, based upon the evidence presented to the Magistrate Judge, the defendant collected or hoarded child pornography. Some courts, including the Second Circuit, have recognized a tendency by child pornographers to hoard child pornography. *See, e.g., United States v. Shields*, 458 F.3d 269, 279 n. 7 (3d Cir. 2006)(stating that "collectors of child pornography rarely, if ever, dispose of their collections"); *United States v. Gourde*, 440 F.3d 1065, 1072 (9th Cir. 2006)(finding that the defendant fit the "collector profile" based upon evidence set forth in warrant application); *United States v. Martin*, 426 F.3d 68 (2d Cir. 2005); *Payne*, 519 F. Supp. 2d at 477 (D.N.J. 2007)(taking judicial notice of the fact that individuals who acquire pornography ordinarily retain it for long periods of time). However, in many of those cases, there was evidence from which to infer that the particular defendant collected or hoarded child pornography. For example, in Martin, the Second Circuit found probable cause for a search warrant based *inter alia* upon an affidavit that "described the characteristics and proclivities of child-pornography collectors,

specifically how they tend to collect such material, store it, and rarely destroy or discard it” and described the defendant’s membership subscription to an illicit e-group. Martin, 426 F.3d at 74-75. Similarly, in Gourde, the Ninth Circuit found ample cause to infer that the defendant was a hoarder or collector of child pornography based upon his pre-paid unlimited subscription to an illicit website. The Circuit found that this “multi-month” unlimited membership to the website provided agents with “near certainty” that his computer contained evidence of multiple images of child pornography.

In this case, however, was no evidence suggesting that this defendant collected or hoarded child pornography. He did not subscribe to any illicit internet publications or e-groups. He did not have a pre-paid membership. There was no evidence indicating that he had “collected” or downloaded many illicit images. In fact, the search warrant application referenced only one known image of child pornography having been downloaded from the defendant’s computer on one occasion. Under those circumstances, the evidence was insufficient to infer that this defendant collected or hoarded child pornography.

Alternatively, the government asks this Court to assume that the illicit image would still be at the defendant’s residence because most people do not replace their computers annually. That is, since it was known that child pornography had been downloaded from an IP address at that residence a year earlier, and since agents had also confirmed that the person using the IP address still lived at the residence, it was proper to assume that the computer onto which the pornography had been downloaded would still be at the residence. Admittedly, this is an exceptionally close case. On the one hand, it is logical to assume that people do not replace their home computers annually. On the other hand, even if it were assumed that most people do not replace their computers annually, the age of the defendant’s computer was unknown to the government and the Magistrate Judge at the time the warrant was issued. It was just as likely that defendant Coon had downloaded the image onto a five-year-old computer as it was that he had downloaded it onto a newly-acquired computer. Although this is a very close case, the Court finds that the totality of the circumstances did not support probable cause to issue the warrant. Where, as here, agents were aware of: (1) only one image containing child pornography that (2) had been downloaded almost a full year before the search warrant was issued and (3) no other circumstances to confirm the likelihood that the computer or child

pornography would still be at the residence nor (4) evidence from which to infer hoarding of child pornography, the Court finds that probable cause was lacking.

(Coon, No.10CR110; Docket No. 43, pages 5-6)

As in Coon, the facts in the instant case distinguish it from Martin and the other “hoarding” cases. Although the search warrant application contains a boilerplate recitation of the “common characteristics” of individuals involved in child pornography, unlike in Martin, there is no evidence in this case of any on-going or repetitive conduct on the part of the suspected user in this case – such as a membership in an illicit e-group. Aside from the alleged single access of the Motherless website on January 16, 2011, the government presented no evidence to suggest that the suspect in this case fits the profile of an individual who hoards and distributes child pornography as suggested by the boilerplate language in the supporting affidavit. Indeed, as noted above, in this respect the instant case is less compelling than Coon inasmuch as the computer at issue in Coon was the *source* of the child pornography, whereas the only information presented in support of the search warrant in the instant case is that the user accessed a website containing child pornography on one day 10-months earlier.

Based upon a review of the totality of the circumstances, probable cause did not exist in support of the October 27, 2011 search warrant.

Good Faith

The government contends that even if the Court were to determine that probable cause was lacking with respect to the October 27, 2011 search warrant, that the search of the defendant’s computer should nevertheless be upheld under the good faith exception to the

exclusionary rule. (Docket No. 34 at page 19).

In Herring v. United States, 555 U.S. 135 (2009), the Supreme Court reiterated that the existence of a Fourth Amendment violation does not automatically mandate suppression. Instead, the Court must also consider whether the officers acted “in objectively reasonable reliance” upon the subsequently invalidated search warrant. Id. at 701. Where there was “objectively reasonable reliance” (often referred to as “good faith”) by the officer, suppression should be denied. Suppression should be the Court’s “last resort, not [its] first impulse.” Id. At 700. In determining whether to grant suppression, courts must balance “the benefits of deterrence” against the social costs of “letting a guilty defendant go free because of the exclusion of possibly probative, but improperly obtained, evidence from use in his prosecution. . . .” See United States v. Julius, 610 F.3d 50, 66 (2d Cir. 2010). Accordingly, [t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence. Herring, 555 U.S. at 144. It is the government’s burden to demonstrate that the good faith exception applies. See United States v. Clark, 638 F.3d. 89 (2d. Cir. 2011).

A warrant issued by a magistrate judge “normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.” Id.; United States v. Leon, 468 U.S. 897, 922 (1984). However, the Second Circuit has identified four situations when the good faith presumption of reasonableness does not apply: (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial

role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable. Clark, 638 F.3d at 100 (quoting United States v. Moore, 968 F.2d 216, 222 (2d Cir. 1992)).

In the instant case, the defendant argues that the Magistrate Judge issuing the search warrant was knowingly misled due to the omission of critical facts in the application and the misrepresentation of other facts contained in the supporting affidavit. (Docket No. 33 at page 15). The record reflects that on May 16, 2011 – five months before the search warrant application in the instant case – Judge Arcara had rejected the government’s arguments that information more than 10-months old and uncorroborated allegations of hoarding were sufficient to constitute probable cause for the search warrant in Coon. The Court finds credible the testimony of Assistant United States Attorney White to the effect that in an email dated March 12, 2011 he asked Ouzer for more information regarding the time frames in the Coon case, and that Ouzer would have understood that the requested information was related to the staleness issue raised by Coon. (Docket No. 30 at 305). Further, the Court credits White’s testimony that he would have advised Ouzer that the Court scheduled a “good faith” hearing relating to the search warrant in Coon because Ouzer would have been a witness in that hearing (had it taken place). (Docket No. 30 at 294). Although White testified that he did not recall getting “into the weeds of what [Judge Arcara’s] decision entailed,” White stated that if he said anything, “it would have been [Judge Arcara] found the warrant stale, but up- but found the good faith exception applied, so he denied the motion to suppress.” (Docket No. 30 at 309). In light of the extended proceedings relating to the suppression issue in Coon and the subsequent discussions between White and Ouzer in

preparation for the anticipated trial in this case during the summer of 2011, the Court finds that such a conversation between White and Ouzer, as proposed by White, must have taken place. The credible evidence in the record reflects that prior to making the application for the search warrant in the instant case, Ouzer was aware that the search warrant in Coon was attacked as being based on stale information and that the Court had determined that probable cause was lacking because the information proffered in support of the search warrant in Coon was stale.

In light of his experience in Coon, Ouzer should have known that the information proffered in support of the search warrant in the instant case was also stale. In addition to staleness, the search warrant application in this case contained misleading information relating to import of the IP logs obtained by HSI. Contrary to the assertion in the search warrant application, and consistent with the credible testimony from Grant, the IP logs do not reflect “more than one incidence of access of thumbnail images by the user” (Government’s exhibit No. 5 at ¶30). Further, the search warrant application improperly suggests that the IP logs reflect that the user accessed 76 separate images on January 16, 2011. (Government’s Exhibit No. 5 at ¶33). Such a representation is not supported by the record in this case. Finally, contrary to the boilerplate language used in the search warrant application (Government’s Exhibit No. 5 at ¶ 35), Ouzer acknowledged that there was no evidence in this case that the target individual in this case was involved in the distribution of child pornography. Again, the only evidence specific to the as of then unidentified user proffered in support of the October 27, 2011 search warrant was the almost 10-month old information that on January 16, 2011, the user of the IP address 67.252.174.8 accessed the Motherless website, and that various thumbnail images were automatically downloaded over a 17-second period into the internet cache of the user’s computer.

In any event, considering the totality of the circumstances, a reasonably well-trained officer, and particularly an officer with Ouzer's experience, would have understood that the limited information obtained from HSI regarding the alleged conduct in January of 2011 would have been stale and insufficient to support a search warrant application in October of 2011. See United States v. Zimmerman, 277 F.3d. 426 (3d Cir. 2002). Further, the search warrant application in this case contained misleading statements that significantly exaggerated the credible import of the information that could be deduced from the IP logs obtained by HSI. While the record in this case does not present strong evidence that the misleading information was intentionally included to deceive the issuing Judge, the totality of the circumstances in this case suggests that the inclusion of the misleading information, along with inapplicable boilerplate language, was grossly negligent. Such conduct does not warrant the application of the good faith exception to the exclusionary rule. Herring, 555 U.S. at 144 ("When the police exhibit 'deliberate,' 'reckless', or 'grossly negligent' disregard for Fourth Amendment rights, the benefits of exclusion tend to outweigh the costs").

In light of the above, it is recommended that the motion to suppress the evidence obtained as a result of the search warrant executed at 73 Henley Road on November 8, 2011 be GRANTED.

Statements

Because the Court finds that the search conducted in this case was illegal, any statements made by the defendant as a result of that search must be suppressed as the fruit of a poisonous tree. United States v. Griswold, 2011 WL 7473466, *11 (W.D.N.Y. 2011)(Of the various fruits

present on the poisonous tree, perhaps the most easily identifiable is a confession resulting from an illegal search).

Conclusion

Based on the above, it is recommended that the motion to suppress be GRANTED.

Pursuant to 28 U.S.C. §636(b)(1), it is hereby ordered that this Report & Recommendation be filed with the Clerk of the Court and that the Clerk shall send a copy of the Report & Recommendation to all parties.

ANY OBJECTIONS to this Report & Recommendation must be filed with the Clerk of this Court within fourteen(14) days after receipt of a copy of this Report & Recommendation in accordance with 28 U.S.C. §636(b)(1), Rules 6(a), 6(e) and 72(b) of the Federal Rules of Civil Procedure, as well as W.D.N.Y. Local Rule 72(a)(3).

FAILURE TO FILE OBJECTIONS TO THIS REPORT & RECOMMENDATION WITHIN THE SPECIFIED TIME, OR TO REQUEST AN EXTENSION OF TIME TO FILE OBJECTIONS, WAIVES THE RIGHT TO APPEAL ANY SUBSEQUENT ORDER BY THE DISTRICT COURT ADOPTING THE RECOMMENDATIONS CONTAINED HEREIN. Thomas v. Arn, 474 U.S. 140, 106 S.Ct. 466, 88 L.Ed2d 435 (1985); F.D.I.C. v. Hillcrest Associates, 66 F.3d 566 (2d. Cir. 1995); Wesolak v. Canadair Ltd., 838 F.2d 55 (2d Cir. 1988); see also 28 U.S.C. §636(b)(1), Rules 6(a), 6(e) and 72(b) of the Federal Rules of Civil Procedure, and W.D.N.Y. Local Rule 72(a)(3).

Please also note that the District Court, on *de novo* review, will ordinarily refuse to consider arguments, case law and/or evidentiary material which could have been, but was not,

presented to the Magistrate Judge in the first instance. See Patterson-Leitch Co. Inc. v. Massachusetts Municipal Wholesale Electric Co., 840 F.2d 985 (1st Cir. 1988).

Finally, the parties are reminded that, pursuant to W.D.N.Y. Local Rule 72.3(a)(3), “written objections shall specifically identify the portions of the proposed findings and recommendations to which objection is made and the basis for such objection and shall be supported by legal authority.” **Failure to comply with the provisions of Rule 72.3(a)(3) may result in the District Court’s refusal to consider the objection.**

So Ordered.

/s/ Hugh B. Scott

United States Magistrate Judge
Western District of New York

Buffalo, New York
April 5, 2013